# The Department of Economic Affairs of the USA

This section will discuss a concrete countermeasure the Department of Economic Affairs of the United States of America can take to mitigate the security risk concerning SPAM. The department can take legal, regulatory and informational measures to mitigate the risk. The countermeasure that is chosen to be elaborated upon is an informational measure. More precisely, to educate individuals and businesses about SPAM. To do this a website is launched on which individuals and businesses can find information about spam and security measures they can implement. The websites main interest is for the users to gain knowledge about cyber security and thus stimulate self-protection.

The costs for the Department of Economic Affairs consist of the research they have to do, costs of hiring cybersecurity specialists to advise them and, promotional costs. The department itself does not have any direct benefits in terms of prevented losses by deploying the countermeasure. However, that is not the aim of the department. The aim is for individuals and businesses to self-protect and thereby prevent losses. This will make SPAM less beneficial for the attackers and reduce the amount of SPAM sent. In addition, the individuals and businesses do not have any direct costs by using the information and the measures stated on the website. If the website is known to them there is no reason for them not to use it. The individuals and businesses do have indirect costs because the website is government run, which means it is paid for by tax revenues. The exact benefits the cybersecurity information website has is not sure, but observations do suggest that such measures work in favour of enhancing security. At least, they increase market transparency for consumers. (Johannes Bauer, 2009)

It is the responsibility of the Department of Economic Affairs to support and improve economic activity as much as possible. Engaging in SPAM causes a lot of economic damage. However, the incentives of the individuals and businesses aren’t sufficient to stop the negative externalities, which is the absence of self-protection. In most cases, the lack of incentive is caused by a misunderstanding the risk of SPAM and the potential loss it can cause. The direct effect of the improved self-protection initiated by the information on the website will reduce the negative externality effect. The reduction of the negative externality effect and therefore some economic losses made by the individuals and businesses incentivize the Department of Economic Affairs to implement the countermeasure.

Bauer, J. M., & Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10), 706-719.